

REMARKS

Applicants respectfully request favorable reconsideration of the above-captioned application as amended.

In this Amendment, claims 1-194 remain pending. Claims 1, 46, 77, 89, 134 and 165 have been amended in terms which more clearly define the present invention. No new matter has been added. Claims 1, 46, 77, 89, 134 and 165 are the independent claims.

In the Office Action, independent claims 1, 46, 77, 89, 134 and 165 and certain of their respective dependent claims were rejected as obvious over U.S. Patent No. 6,714,968 to Prust in view of Official Notice (e.g., separating access control from the content server). Others of the dependent claims, including claim 2, were rejected as obvious over Prust and the Official Notice in view of Slein et al., RFC 2291 (hereinafter "Slein"). Claims 18 and 106 were rejected as obvious over Prust, the Official Notice and Slein, further in view of U.S. Patent No. 6,578,069 to Hopmann et al. Still others of the dependent claims were indicated as being allowable if rewritten in proper independent form.

As shown above, Applicants have amended independent claims 1, 46, 77, 89, 134 and 165 in terms which more clearly define the present invention. Applicants respectfully submit that the independent claims, together with the dependent claims respectively dependent thereon, are patentably distinct from the cited prior art for the following reasons.

Applicants believe that the Examiner is generally familiar with the claims and issues in this case, and therefore Applicants will focus on the specific points of distinction of the claims from the cited prior art.

Independent claims 1 and 89

Applicants will first address independent method claim 1 and its corresponding independent system claim 89. These claims are directed to providing multi user file storage, involving a client node and a remote file server node. Prior to this Amendment, claim 1 recited in step (c):

“maintaining the integrity of the files at the remote file server node by controlling each access to each of the files at the remote file server node so that each access to each of the files at the remote file server node is performed, if at all, on a respective portion of the respective file as most recently updated at the remote file server node,”

In paragraph 6, the Office Action asserts that Prust teaches permitting more than one user of the user group to access the same file of the file group at the remote file server node simultaneously, citing to Fig. 2 and col. 9, lines 5-10, and further asserts that the capability of accessing the same file by multiple clients simultaneously is supported by Prust’s capability of interfacing to WebDAV. The Office Action further asserts that Prust teaches the above-quoted step (c) language, citing to Fig. 3 and col. 6, lines 3-12 and 22-28. Finally, in paragraph 36, the Office Action addresses Applicants’ arguments in the previous Amendment.

As understood by Applicants, the position of the Office Action is as follows:

(1) In Fig. 2, Prust allegedly discloses hardware that could support the features of claim 1, and expressly supports WebDAV.

(2) WebDAV is described by Prust as enabling “accessing the data files within the remote storage area as if the data files were local” (col. 9, lines 9-10).

(3) The present specification says on page 3, lines 7-9 that:

“Local area networks enable sharing at two levels, First, groups of users may simultaneously access files in a common storage space. More importantly, users can contemporaneously or simultaneously access the same file.”

From these points, the Office Action appears to conclude that Prust's system actually provides all local area network file access features, and that this can be extended to the context of the present claims.

Applicants respectfully disagree with this conclusion.

As a first point, Applicants' submit that the teachings of WebDAV must be taken from WebDAV itself, not what Prust says about it. As understood by Applicants, WebDAV describes two types of "locks" that determine the ability of users to share access to a document, i.e., Exclusive Locks and Shared Locks. The Exclusive Lock limits access to a single user. As stated in paragraph 6.1 of WebDAV:

"6.1 Exclusive Vs. Shared Locks

The most basic form of lock is an exclusive lock. This is a lock where the access right in question is only granted to a single principal. The need for this arbitration results from a desire to avoid having to merge results."

On the other hand, the Shared Lock permits multiple users to share access to the document without limitation. As also stated in paragraph 6.1 of WebDAV:

"However, there are times when the goal of a lock is not to exclude others from exercising an access right but rather to provide a mechanism for principals to indicate that they intend to exercise their access rights. Shared locks are provided for this case. A shared lock allows multiple principals to receive a lock. Hence any principal with appropriate access can get the lock.

With shared locks there are two trust sets that affect a resource. The first trust set is created by access permissions. Principals who are trusted, for example, may have permission to write to the resource. Among those who have access permission to write to the resource, the set of principals who have taken out a shared lock also must trust each other, creating a (typically) smaller trust set within the access permission write set.

Starting with every possible principal on the Internet, in most situations the vast majority of these principals will not have write access to a given resource. Of the small number who do have write

access, some principals may decide to guarantee their edits are free from overwrite conflicts by using exclusive write locks. Others may decide they trust their collaborators will not overwrite their work (the potential set of collaborators being the set of principals who have write permission) and use a shared lock, which informs their collaborators that a principal may be working on the resource.”

Thus, WebDAV does not itself provide for merging edits or ensuring that edits are made on a most up-to-date copy of a document when using a Shared Lock for multiple users. Rather, it relies on “trust” so that each user is dependent on the good faith and accuracy of the other users.

The methods and systems in accordance with the present invention as defined in the pending claims are not so limited. They enable multiple users to access the same document while at the same time providing new and effective mechanisms for ensuring that “results” are properly “merged.”

The first of the mechanisms is recited in independent claim 1. Indeed, the Office Action does not address a key limitation of claim 1 that recites this mechanism. Specifically, claim 1 does not merely recite that multiple users have simultaneous access to the same file. Rather, claim 1 recites in step (c), as noted above (emphasis added):

“maintaining the integrity of the files at the remote file server node by controlling each access to each of the files at the remote file server node so that each access to each of the files at the remote file server node is performed, if at all, on *a respective portion of the respective file* as most recently updated at the remote file server node,”

Applicants respectfully submit that they have found no teaching or suggestion in any of the cited references that any (possibly simultaneous) access to a file is on *a respective portion of the respective file*, as opposed to access on the entire file. Nor does the Office Action cite to any such teaching or suggestion in the cited references.

To clarify this claim recitation, which was already in the claim language, Applicants have now amended claim 1 to recite that *the respective portion is less than all of the respective file*. With this clarification, Applicants respectfully submit that independent claim 1 is now clearly seen to be patentably distinct from the cited prior art.

The same clarification has been made in corresponding independent system claim 89, and therefore this claim is also believed to be patentably distinct from the cited prior art.

Independent claims 46 and 134

Applicants will now address independent method claim 46 and its corresponding independent system claim 134. These claims are also directed to providing multi user file storage, involving a client node and a remote file server node, wherein users can access files of a file group at the remote file server node. Prior to this Amendment, claim 46 recited in step (d):

“delegating access control to a particular file of the group of files to an access control node.”

In paragraph 6, the Office Action notes that Prust does not teach this feature, but takes Official Notice that:

“separating access control (e.g., authentication and authorization) from the content server is well known in the art of load sharing or in three-tier content provisioning services, wherein the access control is normally performed at a different node so as to free up the content servers from the burden of qualifying a user.”

Without conceding that this Official Notice remedies the acknowledged deficiency of Prust as a reference against claim 46, Applicants note that the access control of the present invention is not specifically drawn to authentication and authorization, which would merely be directed to ensuring that only proper users are accessing the system. Rather, as stated on page 45, lines 2-5 of the present specification:

“The remote file server node and client nodes maintain the integrity of the group of files on the virtual storage device by ensuring that all accesses to the (master) copies of the files maintained on the virtual storage device occur on the most up to date version of these (master) copies.”

As discussed above, this feature arises from mechanisms that ensure that “results” by multiple users are properly considered and “merged,” and is not found in the prior art.

Applicants specifically submit that this feature of the present invention is neither taught nor suggested by either Prust or the indicated Official Notice. In this regard, although the Office Action in paragraph 6 generally asserts that Prust discloses such a feature, Applicants have not found such a disclosure in any of the cited portions of Prust or in the remainder thereof.

Accordingly, Applicants have amended independent claim 46, as shown above, to recite:

“delegating access control to a particular file of the group of files to an access control node, such that access to the particular file maintained at the remote file server node occurs on a most up to date version of the particular file.”

Applicants respectfully submit that amended independent claim 46 is patentably distinct from the cited prior art.

The same clarification has been made in corresponding independent system claim 134, and therefore this claim is also believed to be patentably distinct from the cited prior art.

Independent claims 77 and 165

Applicants will now address independent method claim 77 and its corresponding independent system claim 165. These claims are also directed to providing multi user file storage, where each user of the pre-subscribed user group may access the same file of the file group at the remote file server node simultaneously.

The Office Action addresses the issue of a public-private key pair in connection with claims 34-36 and 39, and then references this discussion with regard to claim 46. In paragraph 9, the Office Action states:

“Official Notice is taken that encrypting a data file using a public-private key pair and transferring encrypted key for a designated user who only knows the public key (for purpose of decrypting the encrypted key) is well known in the art.”

Applicants respectfully note that the operation described in the Official Notice does not correspond to the operation recited in claim 77. To clarify this point, Applicants have amended claim 77. More specifically, amended claim 77 recites:

“(c) transferring an encrypted key from the remote file server node to a particular client node via a secure channel, the encrypted key being encrypted using an encryption function not known locally at the remote file server node, the key being decryptable using a decryption function not known locally at the remote file server node, the decryption function being also not known locally at any other client node usable by others of the pre-subscribed user group”

Applicants respectfully submit that this step is distinct from, and not suggested by, the Official Notice in the Office Action or described in the cited prior art.

Applicants respectfully submit that amended independent claim 77 is patentably distinct from the cited prior art.

Claim 165 is a system claim that has been amended corresponding to method claim 77. Accordingly, Applicants respectfully submit that independent claim 165 is also patentably distinct from the cited prior art.

The remaining claims depend from a respective one of the independent claims 1, 46, 77, 89, 134 and 165 and partake of the novelty thereof.

In view of the above amendments and remarks, it is respectfully submitted that claims 1-194 are patentably distinct from the cited prior art and are in proper form for allowance. Accordingly, the Examiner is respectfully requested to allow this application and pass this case to issue.

If any fee is due for this filing, please charge the LARGE ENTITY fee therefor to Deposit Account No. 16-2500 of the undersigned.

Applicants' undersigned attorney may be reached by telephone at (212) 969-3314 or by facsimile at (212) 969-2900. Please direct all correspondence to Customer No. 21890 at the address provided below.

Respectfully submitted
PROSKAUER ROSE LLP
Attorneys for Applicants

Date: December 13, 2005

PROSKAUER ROSE LLP
1585 Broadway
New York, NY 10036

Tel: (212) 969-3000

By Abigail Cousins
Abigail F. Cousins
Reg. No. 29,292